SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
P. CRAIG CARDON, Cal Bar No. 168646
ccardon@sheppardmullin.com
JAY T. RAMSEY, Cal Bar No. 273160
jramsey@sheppardmullin.com
ALYSSA SONES, Cal Bar No. 318359
asones@sheppardmullin.com
KEVIN MURPHY, Cal Bar No. 346041
kemurphy@sheppardmullin.com
1901 Avenue of the Stars, Suite 1600
Los Angeles, California 90067-6017
Telephone: (310) 228-3700
Facsimile: (310) 228-3701

Attorneys for Defendant
AFTERSHOKZ, LLC

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, WESTERN DIVISION

ROBERT CONOHAN, individually and on behalf of all others similarly situated;

Plaintiff,

v.

AFTERSHOKZ, LLC, a Texas limited liability company; DOES 1 through 25, inclusive

Defendant.

Case No. 2:24-cv-08786 MWF (Ex)

Hon. Michael W. Fitzgerald

DEFENDANT AFTERSHOKZ, LLC'S NOTICE OF MOTION AND MOTION TO DISMISS PLAINTIFF'S FIRST AMENDED CLASS ACTION COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

[*Filed concurrently with Request for Judicial Notice and Proposed Order*]

Date: November 18, 2024
Time: 10:00 a.m.
Ct. Rm.: 5A

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on November 18, 2024, at 10:00 a.m., or as soon thereafter as the Motion may be heard in Courtroom 5A of the above entitled Court located at 350 West First Street, Los Angeles, California 90012, the Honorable Michael W. Fitzgerald presiding, Defendant Aftershokz LLC will, and hereby does, move the Court for an order dismissing this action in its entirety with prejudice and without leave to amend pursuant to Federal Rule of Civil Procedure 12(b)(6). This Motion is made following the conference of counsel pursuant to L.R. 7-3 which took place on October 9, 2024.

Defendant moves to dismiss the First Amended Class Action Complaint filed by Plaintiff Robert Conohan, under Federal Rule of Civil Procedure 12(b)(6) on the grounds that Plaintiff fails to state a claim upon which relief can be granted.

This Motion is based upon this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, Defendant's Request for Judicial Notice, and the exhibits attached thereto, filed concurrently herewith, and all pleadings and papers in the Court's file, the record and files herein, and upon such oral argument as may be made at the hearing on the Motion and such other evidence as may be admitted at the time of the hearing on the Motion.

Dated: October 18, 2024 SHEPPARD, MULLIN, RICHTER & HAMPTON LLP

By */s/ P. Craig Cardon*
P. CRAIG CARDON
JAY T. RAMSEY
ALYSSA SONES
KEVIN MURPHY

Attorneys for Defendant
AFTERSHOKZ, LLC

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

Plaintiff alleges a violation of California Penal Code section 638.51 ("section 638.51"), which prohibits the use of a "trap and trace device" without a court order. A "trap and trace device" is a "device or process" installed on a person's phone "that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50. In simple terms, a "trap and trace device" is a device that a third party installs on a person's telephone that tells that third party who called that person's phone. Trap and trace devices are used by law enforcement to determine if a suspect is engaging in criminal activity. For example, if law enforcement installed a trap and trace device on Person A's phone, the trap and trace device would tell law enforcement that Person A received a phone call from Person B's phone number.

This case, however, is not about phones, phone calls, a criminal investigation, or a third-party installing anything on Plaintiff's phone. Rather, this case is brought against Defendant Aftershokz LLC ("Aftershokz" or "Defendant"), which operates a website, www.shokz.com, where it sells headphones. Plaintiff alleges that he visited the website and, without his consent, Aftershokz used software created by TikTok, which was installed on Aftershokz's website, to capture record information that his device sent to the website. The software then shared the information with TikTok to learn his identity. Plaintiff alleges that the software is a trap and trace device, and that Aftershokz has violated section 638.51 by installing and using the trap and trace device without a court order.

But the software is not a trap and trace device. A trap and trace device is installed by a third-party on a person's device, without their consent, to learn who is calling that person. Plaintiff, however, alleges that Aftershokz installed the software on *its own website* to learn that Plaintiff had visited the site. This is akin to Person

A using Caller ID on his own phone to learn that Person B is calling him, which is obviously not illegal.

Considering the complete mismatch between Plaintiff's theory and the statute at issue, it is no surprise that this case should be dismissed. ***First***, section 638.51 applies only to telephones, not to a website that captures information sent to it from a visitor's device. This is confirmed by the text, structure, and legislative history of section 638.51. Moreover, applying section 638.51 to a commercial website makes little sense when considering the California Consumer Privacy Act ("CCPA"). The CCPA was enacted *after* section 638.51 and regulates the exact conduct that Plaintiff complains of. Plaintiff's interpretation of section 638.51 would thus undermine the CCPA and lead to absurd results. ***Second***, even if the Court finds that section 638.51 applies to website software, the software that Aftershokz allegedly installed on its website is not a trap and trace device because it purportedly collects the "contents" of a communication. By definition, software that collects the "contents" of a communication is not a trap and trace device. ***Third***, even if the software is a trap and trace device, Aftershokz is exempted from liability under section 638.51 because it is a provider of an electronic communication service. ***Fourth***, Aftershokz acknowledges that two federal district courts have denied a defendant's motion to dismiss a plaintiff's section 638.51 claim. But for the reasons explained in Section III.F, those cases were wrongly decided and are distinguishable. The Motion to Dismiss should be granted.

II. ALLEGATIONS IN THE FIRST AMENDED CLASS ACTION COMPLAINT

Aftershokz is a retailer that sells headphones. (First Amended Class Action Complaint ["FAC"] ¶ 1.) Aftershokz operates a website, www.shokz.com (the "Website") that Plaintiff alleges he visited on January 8, 2024. (*Id.* ¶ 2.) Plaintiff alleges no details about his visit, such as what he did on the Website, whether he purchased a product, or anything else.

Plaintiff alleges that Aftershokz "has installed on its Website software created by TikTok [("TikTok Software" or "Software"]] in order to identify website visitors." (FAC ¶ 11.) According to Plaintiff, when a user visits a website, the user's device generates "electronic impulses" that are sent to the website. (*Id.* ¶¶ 19-20.) On Aftershokz's website, the TikTok Software allegedly captures the "incoming electronic impulses," which constitute "device and browser information, geographic information, referral tracking, and URL tracking" along with "phone number, email, routing, addressing, and other signaling information." (*Id.* ¶¶ 13, 19, 34.) TikTok then matches this information with existing data that it has acquired through its "AutoAdvanced Matching" technology, in an effort to identify the website visitor.[1] (*Id.* ¶ 15.)

While visiting the Website, Plaintiff alleges that Aftershokz used the TikTok Software to identify him. (FAC ¶ 2.) Plaintiff does not allege whether his device is a phone, computer, or something else. Nor does Plaintiff allege what information Aftershokz collected from his device. Nonetheless, Plaintiff alleges that the TikTok Software is a trap and trace device and that Aftershokz gathered the information generated from his device without his knowledge, consent, or a court order in violation of section 638.51. (*Id.* ¶¶ 2, 22-23.)

[1] Plaintiff does not allege that the "AutoAdvanced Matching" technology is a trap and trace device or that the use of the AutoAdvanced Matching technology violates section 638.51. (FAC ¶¶ 18-23, 34 [alleging that Aftershokz violated section 638.51 by using the TikTok Software].) However, during the parties' meet and confer, Plaintiff's counsel stated that the AutoAdvanced Matching technology is also a trap and trace device. To the extent Plaintiff premises his section 638.51 claim on the AutoAdvanced Matching technology, his claim fails for the same reasons as his claim premised on the TikTok Software.

III. THE COURT SHOULD DISMISS THE FIRST AMENDED CLASS ACTION COMPLAINT

A. Legal Standard

A motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6) tests the legal sufficiency of claims asserted in a complaint. A claim should be dismissed where there is either a "lack of a cognizable legal theory" or "the absence of sufficient facts alleged under a cognizable legal theory." *Balistreri v. Pacifica Police Dep't,* 901 F.2d 969, 699 (9th Cir. 1988). A plaintiff must do more than allege "labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A complaint must at least allege sufficient facts "to raise a right to relief above a speculative level." *Id. See also Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Accordingly, "[t]o survive a motion to dismiss, a complaint must plead sufficient factual matter, accepted as true to allow the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *City of Dearborn Heights Act 345 Police & Fire Ret. Sys. v. Align Tech., Inc.*, 65 F. Supp. 3d 840, 849 (N.D. Cal. 2014) (cleaned up).

B. Plaintiff Has Failed To State A Claim Under California Penal Code Section 638.51 Because Trap and Trace Devices Apply Only To Telephone Communications, Not Website Technologies

Trap and trace devices are devices used by law enforcement to track who is calling whom ***by telephone***. They are not devices that relate in any way to tracking on the internet. This is confirmed by the statutory text and structure, the legislative history, the context of California's overall regulatory scheme, and public policy. As a result, section 638.51 does not apply to Aftershokz's alleged use of the TikTok Software.

1. *Statutory text and structure*

When interpreting a statute, the California Supreme Court has instructed courts to "begin with its text" because "statutory language typically is the best and most reliable indicator of the Legislature's intended purpose." *Larkin v. Workers' Comp. Appeals Bd.*, 62 Cal. 4th 152, 157 (2015). If the statute's text "depends on cross-referenced provisions," those provisions are equally indicative of the Legislature's intent. *Id.* at 160. The "text alone," however, "is not dispositive." *Id.* "[T]exual arguments are further bolstered by structural ones—[the statute's] place in the broader structure of the statutory scheme." *Id.*

Starting with the text, section 638.51 states that "a person may not install or use a . . . trap and trace device without first obtaining a court order pursuant to Section 638.52 or 638.53." A "trap and trace device" is a "device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50. While the definition of "trap and trace device" does not expressly state whether it includes general website technologies that capture incoming information from a website visitor's device, the cross-referenced provisions in the statute, sections 638.52 and 638.53, confirm that it does not.

Sections 638.52 and 638.53 permit law enforcement to use a trap and trace device if certain conditions are met. Subsection (d) of section 638.52 details specific information that must be included in a court order authorizing the use of a trap and trace device. Critically, such information includes the ***telephone line*** and ***telephone number*** of the individual that law enforcement is investigating. Indeed, the subsection states that a court order permitting law enforcement to use a trap and trace device must include "[t]he identity, if known, of the person to whom is leased or in whose name is listed ***the telephone line*** to which the . . . trap and trace device

is to be attached." Cal. Penal Code § 638.52(d)(1) (emphasis added). The order must also include "[t]he ***number*** and, if known, physical location of the ***telephone line*** to which the . . . trap and trace device is to be attached." *Id.* § 638.52(d)(3) (emphasis added). Furthermore, subsection (c) again references telephones, stating that information acquired via a trap and trace device shall not include the physical location of the targeted individual "except to the extent that the location may be determined from the ***telephone number***." *Id.* § 638.52(c) (emphasis added).

The multiple references to telephones in sections 638.52 and 638.53 demonstrate that a "trap and trace device" applies only to telephonic communications. If the Legislature had intended, in 2015, for a trap and trace device to encompass communications beyond telephonic communications, it would not have required a court order authorizing the use of a trap and trace device to detail the "number" and "physical location" of a "telephone line." Indeed, the decision to limit sections 638.50-638.53 to telephonic communications was a deliberate choice by the Legislature. For example, in 2016, the Legislature enacted a new provision of CIPA, section 632.01, which prohibits the disclosure of certain confidential communications "in any forum, including . . . *Internet Web sites*." Cal. Penal. Code § 632.01(a)(1) (emphasis added). The Legislature's choice to apply section 632.01 to the internet, but omit similar language from sections 638.50-638.53, demonstrates that the Legislature intended section 638.51 to apply only to telephones. Furthermore, in 2016, one year after enacting sections 638.50-638.53, the Legislature amended section 638.52 to compensate telecommunications providers for assisting law enforcement in installing a pen register or trap and trace device. Cal. Penal Code § 638.52(j). Yet the Legislature chose not to amend section 638.52 to remove the language referencing telephones. What's more, in 2022, the Legislature again amended section 638.52. This time to prohibit a magistrate judge from authorizing the use of a pen register or trap and trace device in certain situations. Cal. Penal. Code § 638.52(m). Again, the Legislature did not

remove the language referencing telephones. Nor did the Legislature amend sections 638.50-638.53 to explicitly state that trap and trace devices applied to internet communications. *See In re The Application of the United States of America for an Order Authorizing the use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. 197, 200 (C.D. Cal. 1995) (explaining that Congress's decision to limit the Federal Wiretap Act's trap and trace provision to telephone lines could "not be assumed to be inadvertent").

In short, there is nothing in the statutory text that suggests that the Legislature intended section 638.51 to apply to a website operator that uses common website technologies to capture incoming information from a website visitor's device.

2. *Legislative history*

In addition to the statutory text, a court may consider the statute's legislative history to determine the Legislature's intent. *Kavanaugh v. W. Sonoma Cty. Union High Sch. Dist.* 29 Cal. 4th 911, 920 (2003) ("In order to ascertain a statute's most reasonable meaning, we often examine its legislative history."). The legislative history of sections 638.50-638.53 further support the conclusion that the Legislature never intended for section 638.51 to apply to commercial websites that capture incoming information from a website visitor's device.

a. Assembly Bill 929

California Penal Code sections 638.50-638.53 were enacted in 2015 as part of a statutory scheme that authorized state and local law enforcement to use trap and trace devices as long as certain conditions were met. (Request for Judicial Notice ["RJN"] Ex. A, p. 1].) According to the legislative history, the purpose of Assembly Bill 929 (now Penal Code sections 638.50-638.53) was "to authorize state and local law enforcement to seek emergency orders for pen registers/trap and trace devices used in telephone surveillance, while requiring as a precondition a standard of evidence higher than under federal law." (RJN Ex. B, p. 4].) The need for the bill arose due to a conflict between federal and state law. Federal law authorized "states

and local law enforcement officers to use pen register and trap and trace devices by obtaining a court order first," but it did "not allow them to obtain an emergency order unless there [was] a state statute authorizing and creating a process for states and local law enforcement officers to do so." (RJN Ex. A, p. 10].) At the time, California did not "have a state statute authorizing the use of pen registers or trap and trace devices." (*Id.*) Thus, local and state law enforcement agencies that utilized trap and trace devices on an emergency basis were technically in violation of federal law. (RJN Ex. B, pp. 5-6].) Assembly Bill 929 sought to remedy that problem by creating a comprehensive statutory scheme that "explicitly authorize[d] state and local law enforcement officers to use pen register and trap and trace devices, including during emergency situations." (*Id.*, p. 6.)

As can be seen from the above, nothing in the legislative history indicates that the Legislature intended section 638.51 to apply to common website technologies that capture incoming information from a website visitor's device. This is further confirmed by the Assembly and Senate bill analyses, which repeatedly describe the statute as one that applies to "telephone surveillance." Indeed, the legislative history repeatedly refers to pen registers and trap and trace devices as tools that law enforcement uses to collect telephone numbers. (*See* RJN Ex. A, p. 10 ["[A]nother tool law enforcement uses is called a ***'trap and trace device' which allows them to record what numbers have called a specific telephone line, i.e. all incoming phone numbers***." (emphasis added)]; *id.*, p. 10 ["Pen registers and track *[sic]* and trace devices track ***incoming and outgoing telephone calls***." (emphasis added)]; *id.*, p. 11 ["any location information obtained by a pen register or a track *[sic]* and trace device is limited to the information that is contained in the ***telephone number***" (emphasis added)]; Ex. B, p. 1 [stating that AB 929 "[a]uthorizes state and local law enforcement agencies to seek an emergency order to use pen registers and trap and trace devices in ***telephone surveillance***" (emphasis added)]; *id.*, p. 5 ["As noted above, pen registers/trap and trace devices are used by law enforcement for

telephone surveillance to record incoming and outgoing ***phone numbers from a tapped line***." (emphasis added)]; Ex. C, p. 1 ["This bill authorizes state and local law enforcement agencies to seek an emergency order to use pen registers and trap and trace devices in ***telephone surveillance*** . . . ." (emphasis added)].) In contrast, the legislative history does not mention websites, IP addresses, website technologies, or an any intent by the Legislature for website visitors like Plaintiff to use the statute as a vehicle to enforce their privacy rights through civil litigation. If section 638.51 was meant to apply to commercial websites that capture incoming information from a website visitor's device – and therefore to consumers that visit such websites – the legislative history would have at least acknowledged that, particularly given the internet's widespread use by 2015. But it does not.

b. Assembly Bill 1924

If Assembly Bill 929 wasn't enough, the Legislature reaffirmed in Assembly Bill 1924 that section 638.51 was meant to apply only to telephones. Assembly Bill 1924 was enacted into law one year after Assembly Bill 929. Assembly Bill 1924 primarily amended California's Electronic Communication Privacy Act ("ECPA") (Cal. Penal Code §§ 1546 et seq.), which allows the government to compel the production of "electronic information" under certain circumstances, such as if the government obtains a search warrant or a wiretap order. (RJN Ex. F, pp. 6-9.) The ECPA did not, however, expressly permit the government to compel the production of "electronic information" pursuant to a pen register or trap and trace order under section 638.52. (*Id.*) Because of this, the government would have to obtain a search warrant in order to use a pen register or trap and trace device. Assembly Bill 1924 amended the ECPA to ensure the government could compel the production of "electronic information" pursuant to a pen register and trap and trace order under section 638.52, rather than a search warrant. (*Id.*)

Critically, the bill analyses of Assembly Bill 1924 explained that the ECPA applied to pen registers and trap and trace devices because the ECPA's "definition[]

of electronic communication . . . include[s] ***the call detail records*** that are captured by a pen register/trap and trace device." (RJN Ex. F, p. 7 (emphasis added).) In other words, the bill analyses confirm that the "electronic information" that the ECPA permits the government to collect from pen registers and trap and trace devices is phone numbers, not information derived from the internet, like browser information or IP addresses. Importantly, both the ECPA and section 638.50 (which defines pen registers and trap and trace devices) use the term "electronic communication," suggesting that when the Legislature defined a trap and trace device as a device that "identif[ies] the source of a . . . electronic communication" it meant communications via telephone, not the internet. This is further confirmed by the bill analyses' repeated references to pen registers and trap and trace devices as devices that collect phone numbers. (*See* RJN Ex. D, p. 6 ["Pen registers and track [*sic*] and trace devices generally track incoming and outgoing ***telephone calls***." (emphasis added)]; *id.*, p. 7 ["A 'trap and trace device' records what ***numbers had called a specific telephone***, i.e., all ***incoming phone numbers***." (emphasis added)]; Ex. E, p. 1 ["pen register/trap and trace-device[s] . . . are ***telephone surveillance devices used to record incoming and outgoing phone numbers***" (emphasis added)].)

In sum, nothing in the legislative history suggests that the section 638.51 applies beyond telephone communications.

3. *California Consumer Privacy Act*

When interpreting a statute, courts "endeavor to harmonize it with other enactments to the extent possible." *Lexin v. Superior Court*, 47 Cal. 4th 1050, 1095 (2010). Indeed, when possible, "courts must construe a statute so as not to conflict with the other legislative enactments." *Nat'l Indem. Co. v. Garamendi*, 233 Cal. App. 3d 392, 405 (1991). Here, Plaintiff's interpretation of section 638.51 cannot be reconciled with the California Consumer Privacy Act ("CCPA").

Enacted in 2018, three years after section 638.51, the CCPA regulates the collection of "personal information" by businesses. Cal. Civ. Code § 1798.100 et seq. The definition of "personal information" is broad: "'Personal Information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer." Cal. Civ. Code § 1798.140(v)(1). In addition, personal information specifically includes: (1) "Identifiers such as . . . email address"; (2) "Internet or other electronic network activity information, including . . . a consumer's interaction with an internet website application"; and (3) "Geolocation data." Cal. Civ. Code § 1798.140(v)(1)(A), (F), (G). Importantly, the CCPA permits businesses to collect personal information (and therefore all the information identified above) as long as the business complies with the CCPA. *See* Cal. Civ. Code § 1798.100(c). And the CCPA grants consumers the "right to request that a business delete any personal information about the consumer that the business has collected from the consumer." Cal. Civ. Code § 1798.105.

Taking into consideration the CCPA, Plaintiff's interpretation of section 638.51 makes little sense. If, according to Plaintiff, section 638.51 prohibits businesses from collecting any information generated from a website visitor's device that identifies the website visitor, including email addresses, geolocation data, and a visitor's interaction with the website (i.e., the exact information that Plaintiff alleges the TikTok Software collects (FAC ¶¶ 13, 19, 34)), why did the Legislature permit businesses to collect such information and afford consumers the right to request that businesses delete such information? The only logical interpretation is that section 638.51 does not apply to website technologies that

capture incoming information from a website visitor's device. For this additional reason, Plaintiff's proffered interpretation of section 638.51 is incorrect.[2]

4. *Public policy*

After examining the statutory text, structure, and legislative history, if the statute's meaning is still uncertain, "it is appropriate [for a court] to consider the consequences that will flow from a particular interpretation." *Copley Press, Inc. v. Superior Court*, 39 Cal. 4th 1272, 1291 (2006) (quotations omitted). The California Supreme Court has instructed that "where more than one statutory construction is arguably possible," the Court's "policy has long been to favor the construction that leads to the more reasonable result." *Id.* "This policy derives largely from the presumption that the Legislature intends reasonable results consistent with its apparent purpose." *Id.* Thus, a court should "select the construction that comports most closely with the Legislature's apparent intent, with a view to promoting rather than defeating the statutes' general purpose, and to avoid a construction that would lead to unreasonable, impractical, or arbitrary results." *Id.*

Interpreting the statute as Plaintiff proposes would lead to unreasonable results that the Legislature never contemplated. If, as Plaintiff alleges, a website that uses a website technology to capture incoming information from a website visitor's device is using a trap and trace device, then every website that obtains such information would be subject to criminal liability. A website operator cannot obtain a court order permitting it to use such technology because it is not a peace officer. *See* Cal. Penal Code §§ 638.52, 638.53. And a website operator cannot obtain a website visitor's consent to use the technology because, under section 638.51, consent is a defense only for the provider of an electronic communication service. Cal. Penal Code § 638.51. Although Aftershokz argues that it is a provider of an

[2] The CCPA also does not mention pen registers, trap and trace devices, or section 638.51. If, as Plaintiff alleges, section 638.51 regulates the collection of the same information as the CCPA, one would think that the CCPA would acknowledge that.

electronic communication service (*see infra* Section III.D), if the Court disagrees, Plaintiff's consent would not shield Aftershokz from liability. Accordingly, under Plaintiff's interpretation (and assuming that Aftershokz is not an electronic service provider), every website operator that uses common website technologies would be liable. That cannot be what the Legislature intended when it enacted section 638.51, especially because neither the statute itself nor the legislative history ever mentions the internet, websites, or website technologies. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2009) ("The Supreme Court has long warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants.").

5. *The statute must be construed in Defendant's favor*

To the extent there is any doubt about the proper interpretation of section 638.51, the Court must construe the statute in Aftershokz's favor because (1) the statute is penal in nature and created new liability; and (2) the rule of lenity requires criminal statutes, even when used as the basis for a civil claim, to be construed in the defendant's favor.

First, statutes that carry statutory penalties that are penal in nature "should receive a strict construction" in favor of defendants. *Saracco Tank and Welding Co. v. Platz*, 65 Cal. App. 2d 306, 315 (1944). This is especially true where a statute creates a ***new*** statutory liability, as opposed to amending an old statute or codifying a common law offense. *Tos v. Mayfair Packaging Co.*, 160 Cal. App. 3d 67 (1984); *Weber v. Pinyan*, 9 Cal. 2d 226 (1937). Here, section 638.51 is penal because the provision that imposes a penalty for a violation of section 638.51, section 637.2, does so without regard to compensation for any actual loss suffered. Cal. Penal Code §§ 637.2(a), (c) (a successful civil claimant is entitled to "[f]ive thousand dollars ($5,000)" without ***any*** proof of actual damages); *Hale v. Morgan*, 22 Cal. 3d 388, 397-99 (1978) (Civil Code § 789.3, which imposes a mandatory penalty of $100 per day and does not permit the trier of fact discretion in fixing the penalty, is

penal in nature); *Hypertouch v. Valueclick, Inc.*, 191 Cal. App. 4th 1209, 1243 (2011). Further, the California Supreme Court recognized that section 637.2 "explicitly created a ***new***, statutory private right of action, authorizing any person who has been injured by any violation of the invasions-of-privacy legislation to bring a civil action. . . ." *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95, 115-16 (2006). Indeed, the statute's location in the Penal Code itself is sufficient to suggest that it is penal in nature. *See People v. Moon*, 193 Cal. App. 4th 1246 (2011) (giving "considerable weight" to fact that statute falls within a title of the Penal Code when construing statute).

Second, section 638.51 must be construed in Defendant's favor because the rule of lenity requires courts to construe criminal statutes in favor of defendants even where, as here, those criminal statutes are used as the basis for a civil claim. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) ("Because we must interpret the [criminal] statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies."); *People v. Mobile Oil Corp.*, 143 Cal. App. 3d 261 (1983) (explaining that the rule of lenity applies "even when the underlying action is civil in nature."). The California Supreme Court has reaffirmed this rule, noting that, under the rule of lenity, "a court must generally interpret an ambiguous criminal statute in the defendant's favor." *See People v. Mutter*, 1 Cal. App. 5th 429, 436 (2016).

As a result, to the extent there is any doubt about the proper interpretation of section 638.51, the above doctrines compel the Court to find in favor of Aftershokz.

C. Even If Website Technologies Can Be Trap And Trace Devices, Plaintiff's Claim Still Fails Because The TikTok Software Is Not A Trap And Trace Device

Under section 638.50, a trap and trace device "captures the incoming electronic or other impulses . . . or other dialing, routing, addressing, or signaling information . . . *but not the contents of a communication*." Cal. Penal. Code

§ 638.50 (emphasis added). Thus, according to the statutory text, if the device collects the contents of a communication, it is not a trap and trace device.

Courts analyzing CIPA claims use the Federal Wiretap Act's definition of "contents." *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021). Under the Federal Wiretap Act and CIPA, the "contents" of a communication "refer[] to the intended message conveyed by the communication, and do[] not include record information regarding the characteristics of the message that is generated in the course of the communication." *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). Courts have held that a video recording of a website visitor's interaction with a website are "contents" of a communication. *See Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 518 (C.D. Cal. 2021) (holding that the defendant had intercepted the contents of the plaintiff's communications by "recording . . . a video of Plaintiff's interactions with Nike's website"); *Tanner v. Acushnet Co.*, No. 23-cv-00346, 2023 WL 8152104, at *3 (C.D. Cal. Nov. 20, 2023) (holding that "a video playback that allows the Session Replay Provider and its client to watch the plaintiff's entire session interacting with the site" constituted the "contents" of a communication).

Here, Plaintiff alleges that the TikTok Software captures "***images of website user's interests***" on "virtually every page of Aftershokz's website." (FAC ¶ 16 [emphasis added].) Thus, as alleged, the Software collects the contents of a communication because it permits Aftershokz and TikTok to view each page that a website user visits on the Website. (*Id.* ¶ 17 ["The Aftershokz website instantly sends communications to TikTok . . . every time a user clicks on a page."].) As a result, Plaintiff's claim must be dismissed.[3]

[3] For the same reasons, the AutoAdvanced Matching technology is not a trap and trace device. Plaintiff alleges that the AutoAdvanced technology collects a user's "name, date of birth, and address," which courts have held constitutes the "contents"

D. Plaintiff Has Also Failed To State A Claim Because Defendant Is Exempted From Liability As A Provider Of An Electronic Communication Service

Even if the TikTok Software is a trap and trace device, Aftershokz is not liable because section 638.51(b) permits it to use a trap and trace device on its own website. Caselaw analyzing whether Caller ID is a trap and trace device provides a useful analogy. Caller ID identifies incoming telephone numbers, just as the TikTok Software allegedly identifies incoming information about a visitor's device. In the 1990s, courts and regulatory agencies applying laws identical to California's section 638.51 had to grapple with whether Caller ID – a new technology at the time – was a trap and trace device, and thus illegal. While courts and regulatory agencies held that Caller ID was a trap and trace device, they, nonetheless, concluded that the use of Caller ID was legal. *See Ohio Domestic Violence Network v. PUC of Ohio*, 638 N.E.2d 1012, 1020 (Ohio 1994) (hereinafter "*Ohio Domestic*"); *S. Bell Tel. & Tel. Co. v. Hamm*, 409 S.E.2d 775 (S.C. 1991); *Wis. Pro. Police Ass'n v. PSC*, 555 N.W.2d 179 (Wis. Ct. App. 1996) (hereinafter "*Wisconsin Professional*"); *In re Rules and Policies Regarding Calling No. Identification Serv.—Caller ID*, 9 F.C.C. Rcd. 1764 (1994) (hereinafter "*FCC Decision*").

For example, in the *FCC Decision*, the Federal Communication Commission ("FCC") considered whether Caller ID violated the trap and trace provision of the Federal Wiretap Act. 9 F.C.C. at 1774. The Federal Wiretap Act prohibits the installation and use of a trap and trace device without a court order. But the Federal Wiretap Act provides an exception: it permits (1) the "provider of electronic or wire communication service" (2) to use or install a trap and trace device (3) where "the user of that service" (4) consents. *Id.* at 1780; *see also* 18 U.S.C. § 3121(b). While

---

of communications. *See Price v. Carnival Corp.*, 712 F. Supp. 3d 1347, 1360 (S.D. Cal. 2024).

the FCC concluded that Caller ID was a trap and trace device, it held that a telephone company that provided Caller ID to a telephone subscriber fell within the Act's exception. *Id.* at 1775, 1780. The FCC first held that a telephone company was a "provider of electronic or wire communication service." *Id.* Second, the FCC reasoned that the telephone company used or installed the trap and trace device on a subscriber's telephone. *Id.* Third, the FCC reasoned that the telephone company had to obtain consent only from the "relevant user" of its services to use the trap and trace device. *Id.* The "relevant user" was the telephone subscriber "whose incoming calls are being trapped and traced, *not* those subscribers whose outgoing calls happen to be identified by such device." *Id.* (emphasis added). Fourth, the FCC held that the telephone subscriber, i.e., the "relevant user," consented to the trap and trace device by paying for the Caller ID service. *Id.* Accordingly, the telephone company had not violated the Federal Wiretap Act. *Id.*; *see also Ohio Domestic*, 638 N.E.2d at 322 (holding the same); *Wisconsin Professional*, 555 N.W.2d at 80 ("It is consistent with the [Federal Wiretap Act's] purpose to require only that the Caller ID subscriber consent to the trap and trace device"); *Hamm*, 409 S.E.2d at 73-74 (holding the same as to South Carolina's similar trap and trace law and explaining that the telephone company need only obtain the consent of the person being called).

Importantly, California's section 638.51(b) contains the same exact exception as the Federal Wiretap Act. *Compare* 18 U.S.C. § 3121(b) (stating that an electronic service provider may use a trap and trace device where the consent of the user is obtained) *with* Cal. Penal Code § 638.51(b) (same). Thus, for the same reasons that the FCC and other courts held that a telephone company is not liable for using a trap and trace device when it provides Caller ID to its subscribers, Aftershokz is not liable for installing and using the TikTok Software on its website. First, like a telephone company, Aftershokz is the provider of an "electronic communication service" – here, its website. (FAC ¶ 11.) Like a telephone company

that provides the telephonic means for two individuals to converse, Aftershokz owns and operates its website, which provides the means for its customers to communicate with it. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876 (9th Cir. 2002) (holding that under the Federal Wiretap Act a "website fits the definition of 'electronic communication'"). Second, Aftershokz installed and used the trap and trace device on its website. (FAC ¶ 11.) Third, Aftershokz is a user of its website. It uses the Website to sell products and communicate with its customers. And it is Aftershokz, not Plaintiff, that is the "the relevant 'user'" of the Website because the TikTok Software is installed and used on its website, not Plaintiff's device. *FCC Decision*, 9 F.C.C. at 1774. Fourth, as the relevant user of its website, Aftershokz consented to the installation and use of the TikTok Software when it chose to install the Software on its website. (FAC ¶ 11.) Accordingly, Aftershokz falls within section 638.51(b)'s statutory exception. As such, it was permitted to install and use the TikTok Software on its website and is therefore not liable.[4]

E. Plaintiff Fails To Plead That Aftershokz's Use Does Not Fall Within Other Permissible Uses Under Section 638.51(b)

Plaintiff has also failed to plead that any of the other express statutorily permissible purposes for utilizing a trap and trace do not apply. Rather, he pleads facts that essentially establish that the collection of the information in question is subject to those permissible purposes.

Section 638.51(b) contains a list of permissible uses of a trap and trace device. These are not affirmative defenses but are a part of the statute identifying permissible uses of anything that would otherwise qualify as trap and trace device.

[4] This analysis would of course change if Plaintiff alleged that Aftershokz installed the TikTok Software on *his device*. In that case, Aftershokz would no longer be the "relevant user," and Aftershokz would have to obtain Plaintiff's consent before installing and using the trap and trace device. But Plaintiff does not allege this. As the operator and user of its website, Aftershokz has the right to install the TikTok Software on its site.

In other words, the statutory restrictions on use of a trap and trace have parameters (found in the statute itself). By simply claiming that the challenged technology is a trap and trace, it does not follow that a violation of section 638.51 has occurred. Plaintiff must plead, with facts not conclusions, that the alleged conduct is not just a trap and trace, but that it also falls outside the permissible uses within the statute. Plaintiff has not even attempted to do this.

Here, the allegations in the FAC, indicate that the challenged technology, basically a cookie, falls within the permissible uses of a trap and trace device. A user comes to a website with essentially one piece of information, an IP address. All of the items Plaintiff claims are sent to TikTok are pieces of information that are derived from cross referencing the IP address with other information. Though the FAC is vague (a problem in and of itself), it is basically challenging the collection of an IP address by a cookie. However, it is common practice for website operators, which by their nature are owners of a communications service – the website, to collect and use IP addresses for fraud prevention and cybersecurity purposes. For example, sites may block certain blacklisted IP addresses, or block addresses from IP addresses from countries known for excessive hacking activity, or identify denial of service attacks and other malicious activity by analyzing the IP address activity on the site. Each of these activities falls within the permissible conduct under section 638.51(b)(2) ("To protect the rights or property of the provider"), (b)(3) ("To protect users of the service from abuse of service or unlawful use of the service" such as denial of service and data breaches), (b)(4) ("To record the fact that a wire or electronic communication was initiated or completed to protect the provider . . . or a user of that service from fraudulent, unlawful, or abusive use of the service," again, such as denial of service attacks or data breaches). Plaintiff fails to plead that Aftershokz does not use the allegedly collected information for these purposes, and the core of Plaintiff's allegations lead to the conclusion that it does.

F. The Court Should Not Follow *Moody v. C2 Educational Systems Inc.* And *Greenley v. Kochava, Inc.*

Plaintiff will likely rely on *Moody v. C2 Educational Systems Inc.*, No. 24-cv-04249, 2024 WL 3561367 (C.D. Cal. July 25, 2024) and *Greenley v. Kochava, Inc.* No. 22-cv-01327, 2023 WL 4833466 (S.D. Cal. July 7, 2023) to support his claim. (FAC ¶ 22.) The Court, however, should not follow either case.

In *Moody*, the district court held that software installed on a defendant's website, which captured information from the plaintiff's device, constituted an illegal use of a trap and trace device under section 638.51. 2024 WL 3561367, at *1. There, like here, the plaintiff alleged that the defendant installed the TikTok Software on its website and used the Software to collect his information. *Id.* The *Moody* court's analysis was incomplete and incorrect. ***First***, as to the court's statutory interpretation analysis as to whether trap and trace devices can apply to anything other than telephones, the court failed to consider sections 638.50-53's legislative history, which, as explained, states multiple times that trap and trace devices apply only to telephones. The court also did not consider that applying section 638.51 to website technologies does not make sense in light of the CCPA, which the Legislature enacted *after* section 638.51, and which directly addresses the collection of personal information by websites. Nor did the court consider the public policy implications of its ruling. ***Second***, as to its consent analysis, the court failed to explain why the website visitor must provide consent for the website's decision to install a trap and trace device *on its website*. The court's reasoning would effectively outlaw Caller ID, requiring that a telephone company first obtain the consent of every possible person that may call a telephone subscriber that has installed Caller ID. That conclusion is directly contradictory to the FCC's reasoning and the holdings of multiple state supreme courts. ***Third***, as to the contents argument, the court did not consider the argument that Aftershokz makes in this case – that Plaintiff has alleged that the TikTok Software captures the "images" of every

page a website user visits on the Website. Moreover, the court incorrectly held that if a trap and trace device collects both record information and content information, the device still meets section 638.50's definition of a trap and trace device. Section 638.50 explicitly states that a trap and trace device does not collect "the contents of a communication." Cal. Penal. Code § 638.50. Thus, if website software collects both record information and contents, it is not a trap and trace device. For these reasons, the Court should not follow *Moody*.

For many of the same reasons, the Court should not follow *Greenley*. There, the district court held that "a private company's surreptitiously embedded software installed in a [plaintiff's] telephone" could "constitute a pen register" under section 638.51. 2023 WL 4833466, at *15. *Greenley* is nothing like this case because it concerned the installation of a device on the plaintiff's phone (not alleged here), which the plaintiff alleged was a pen register (not alleged here). Moreover, like the *Moody* court, the *Greenley* court's analysis of the text of section 638.51 is incomplete. The court failed to analyze sections 638.52 and 638.53. Additionally, the court failed to analyze the legislative history, CCPA, or any of the public policy consequences of its interpretation of section 638.51. In short, like *Moody*, the *Greenley* court failed to conduct a fulsome analysis of section 638.51. Accordingly, this Court should not follow its reasoning.

IV. CONCLUSION

For the foregoing reasons, the Court should grant the Motion and dismiss the First Amended Class Action Complaint without leave to amend.

Dated: October 18, 2024 SHEPPARD, MULLIN, RICHTER & HAMPTON LLP

By */s/ P. Craig Cardon*
P. CRAIG CARDON
JAY T. RAMSEY
ALYSSA SONES
KEVIN MURPHY

Attorneys for Defendant
AFTERSHOKZ, LLC

L.R. 11-6.1 Certificate of Compliance

The undersigned, counsel of record for Defendants, certifies that this brief contains 6,962 words, which complies with the word limit of L.R. 11-6.1.

Dated: October 18, 2024 SHEPPARD, MULLIN, RICHTER & HAMPTON LLP

By */s/ P. Craig Cardon*
P. CRAIG CARDON
JAY T. RAMSEY
ALYSSA SONES
KEVIN MURPHY

Attorneys for Defendant
AFTERSHOKZ, LLC